UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,137	08/11/2000	Michel Maillard	11345.023001	8272

22511 7590 03/25/2004

OSHA NOVAK & MAY L.L.P.
1221 MCKINNEY STREET
HOUSTON, TX 77010

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	9

DATE MAILED: 03/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/622,137	MAILLARD ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-25 are pending in this office action.

2. Applicant arguments filed February 27, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claims 1 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Jacques (French Patent No. 2,732,537).

Regarding claim 1, Jacques teaches a method of recording transmitted digital data:

- In which transmitted digital information is encrypted by a recording encryption key (E (NE)) and stored by a recording means on a recording support medium (page 7, line 21 through page 8, line 16) and
- Characterized in that an equivalent of the recording encryption key (E (NE)) is encrypted by a recording transport key (RT (A)) and stored on the support medium together with the encrypted information (page 6, lines 10-20).

Regarding claim 21, Jacques teaches a recording means comprising:

- A security module for encrypting transmitted digital information by a recording encryption key (E (NE)) for storage on a recording support medium (page 7, line 21 through page 8, line 16) and
- Characterized in that the security module is further adapted to encrypt the recording encryption key (E (NE)) by a recording transport key (RT (A)) for storage on the support medium (page 6, lines 10-20).

Claims 1-9, 10, 12, 14-18, and 21-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Tsuria (U.S. Patent No. 6,178,242).

Regarding claim 1, Tsuria teaches a method of recording transmitted digital data:

- In which transmitted digital information is encrypted by a recording encryption key (E (NE)) and stored by a recording means on a recording support medium (figure 2, reference number 145) and
- Characterized in that an equivalent of the recording encryption key (E (NE)) is encrypted by a recording transport key (RT (A)) and stored on the support medium together with the encrypted information (figure 2, reference number 175).

Regarding claim 2, Tsuria teaches the information encrypted by the recording encryption key (E (NE)) comprises control word information (CW) usable to descramble

a scrambled data transmission also recorded on the support medium (column 6, line 65 to column 7, line 1).

Regarding claim 3, Tsuria teaches the recording encryption key (E (NE)) and/or recording transport key (RT (A)) are stored on a portable security module associated with the recording means (column 8, lines 52-59).

Regarding claim 4, Tsuria teaches the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means (column 6, lines 57-62).

Regarding claim 5, Tsuria teaches the decoder is associated with a portable security module used to store transmission access control keys (KO (NS), KO' (Op1, NS) etc.) used to decrypt the transmitted encrypted information (column 7, lines 48-56).

Regarding claim 6, Tsuria teaches:

- The recording encryption key (E (NE)) and/or recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) (column 7, lines 58-64) and
- The transmission access control keys (KO (NS), KO' (Op1, NS) etc.) function in accordance with a second encryption algorithm (CA) (column 8, lines 24-28).

Regarding claim 7, Tsuria teaches the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means (figure 2, reference number 145 transmitted to 175).

Regarding claim 8, Tsuria teaches the recording transport key (RT (A)) is preferably encrypted by a further encryption key (KO (NSIM)) prior to being communicated to the recording means (figure 2, reference number ECM KEY).

Regarding claim 9, Tsuria teaches a central access control system communicates transmission access control keys (KO (NS), KO' (Op 1, NS) etc.) to the recording means (figure 1, reference number 110).

Regarding claim 10, Tsuria teaches the transmission access control keys (KO (NS), KO' (Op1, NS) etc.) are communicated to a portable security module associated with the recording means (figure 1, reference number 120).

Regarding claim 12, Tsuria/ teaches central access control system preferably encrypts the broadcast access control keys (KO (NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means (figure 2, reference number TECM KEY).

Regarding claim 14, Tsuria teaches:

- Using a decoder means and associated security module and a recording means and associated security module (figure 1, reference numbers 110 and 120, and column 6, lines 63-65) and
- In which a copy of the recording transport key (RT (A)) is stored in the security module associated with the decoder means and/or the security module associated with the recording means (column 8, lines 52-59).

Regarding claim 15, Tsuria teaches the recording transport key (RT (A)) is generated by either the recording security modules or decoder security module and communicated to the other security module (figure 2).

Regarding claim 16, Tsuria teaches the recording transport key (RT (A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (KO (NS)) to that other security module (column 8, lines 17-28).

Regarding claim 17, Tsuria teaches the decoder security module and recording security module (52) carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization (column 8, lines 17-28).

Regarding claim 18, Tsuria teaches the mutual authorization step is carried out using, inter alia, an audience key KI (C) known to both security modules (30,52) (column 8, lines 17-28).

Regarding claim 21, Tsuria teaches a decoder means including a security module adapted to store a copy of the recording transport key (RT (A)) (figure 1, reference numbers 110 and 120).

Regarding claim 22, Tsuria teaches a decoder means including a security module adapted to descramble transmitted information using one or more transmission access keys (KO (NS), KO' (Op, NS) etc.) prior to re-encryption by a session key (K3 (NSIM)) for subsequent communication to a recording means (figure 3, and column 9, lines 57-65).

Regarding claim 23, Tsuria teaches a portable security module comprising at least a copy of the recording transport key (RT (A)) (figure 1, reference number 120, and column 7, lines 47-56).

Regarding claim 24, Tsuria teaches a recording means comprising:

- A security module for encrypting transmitted digital information by a recording encryption key (E (NE)) for storage on a recording support medium (figure 2, reference number 145) and

- Characterized in that the security module is further adapted to encrypt the recording encryption key (E (NE)) by a recording transport key (RT (A)) for storage on the support medium (figure 2, reference number 175).

Regarding claim 25, Tsuria teaches a portable security module comprising recording encryption key (E (NE)) for encryption of transmitted digital information for subsequent recording and a recording transport key (RT (A)) for encryption of the recording encryption key for subsequent recording (column 8, lines 17-28).

Claim Rejections - 35 USC § 103

5. Claims 11, 13, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (U.S. Patent No. 6,178,242) in view of Park (European Patent No. 714,204).

Regarding claim 11, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

Park teaches the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption

of the information by the recording encryption key (E (NE)) and storage on the support medium (see page 8, lines 20-22 of Park).

It would have been obvious to combine the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium, as taught by Park, to the method of Tsuria. It would have been obvious to combine the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium, as taught by Park, to the method of Tsuria because the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium would properly restore the encrypted transmission keys to a clear state so that the key can be used to further encrypt the information in the recording means.

Regarding claim 13, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request of authentification by the recording means using a key (KO (NSIM)) unique to that recording means.

Park teaches the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request being authenticated by the recording means using a key (KO (NSIM)) unique to that recording means (see page 8, lines 40-45 of Park).

It would have been obvious to combine the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means, as taught by Park, to the method of Tsuria. It would have been obvious to combine the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means, as taught by Park, to the method of Tsuria because the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means would provide a secure way for the recording means to request keys as needed from the central access control system.

Regarding claim 19, Tsuria teaches all of the subject matter of claims 1 and 14, as discussed above. However, Tsuria does not disclose:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and
- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

Park teaches:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form (page 8, lines 10-19) and
- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)) (page 8, lines 20-22).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session

key to decrypt the information prior to encryption by the recording transport key, as taught by Park, to the method of Tsuria.

It would have been obvious to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key, as taught by Park, to the method of Tsuria because the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form would allow the security module to properly decrypt the encrypted data for proper restoration of the signal.

A session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key would secure the clear signal again before transmission to the recording device, thus making the secure digital recording device more secure.

Regarding claim 20, the combination of Tsuria/Park teaches the session key (K3 (NSIM)) is generated by the decoder security module or recording means security module and communicated to the other module in encrypted form using an encryption

key (KO (NS)) uniquely decryptable by the other security module (see column 8, lines 17-28 of Tsuria).

Response to Arguments

6. Applicant amends claims 1, 7, 13, 17, 18, 24, and 25.

7. Applicant argues:

   a. Independent claim 1 is not taught by Jacques to include "that an equivalent of the recording encryption key is encrypted by a recording transport key and stored on the support medium together with the encrypted information" (page 13, third paragraph).

   b. Independent claim 1 is not taught by Tsuria to include "that an equivalent of the recording encryption key is encrypted by another key, namely, a recording transport key and stored on the support medium together with the encrypted information" (page 14, second paragraph).

   c. Dependent claims are allowable based on their dependency on independent claim 1 (page 15, last paragraph).

Regarding argument (a), examiner disagrees with applicant. The equivalent of the recording encryption key is encrypted by a recording transport key as shown on page 6, lines 10-20. Specifically, it states that the exploitation key *Cex* is also enciphered by an encipherer Ch_2 for transmission. *Cex* is used as the recording

transport key to transmit an equivalent of the recording encryption key. Then the contents are recorded on a digital recorder (fig. 3, ref. num 17).

Regarding argument (b), examiner disagrees with applicant. The TECM (equivalent) of the recording encryption key (ECM key) is encrypted by another key, namely, a recording transport key (TECM key) and stored on the support medium together with the encrypted information (fig. 2, ref. num 150). Because the CW is associated with each respective ECM, the CW itself can be used as the recording encryption key. With that said, both the ECM (i.e. CW) and the TECM with scrambled data are stored on the recording medium, the TECM being an equivalent of the ECM (i.e. CW).

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand as rejected.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Brandon Hoffman

BH
3/18/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100